

2.2 Well-Definedness, and the Arithmetic of the Integers

Section 2.1 built $\mathbb{Z}$ as the set of classes of $\sim$ on $\mathbb{N} \times \mathbb{N}$, and gave each integer a normal form (Proposition 2.1.2). The integers cannot yet be added. Every operation on classes will be defined by a formula on representatives, and *Sets, Relations, and Cardinality*, Section 2.5 showed what can go wrong: a formula that gives two answers for one class (*Sets, Relations, and Cardinality*, Example (A rule on classes that is not a function)). This section proves, once and for all, the lemma that says when such a formula defines a function. It then uses the lemma for the sum, product and negative of integers, and finds a copy of $\mathbb{N}$ inside $\mathbb{Z}$.

2.2.1 Definitions through representatives

In *Sets, Relations, and Cardinality*, Section 2.5 the addition of $\mathbb{Z}/n$ was defined by $[a] + [b] := [a + b]$, and *Sets, Relations, and Cardinality*, Proposition 2.5.5 checked that the right side depends only on the classes, not on the integers a and b used to name them. In *Sets, Relations, and Cardinality*, Example (A rule on classes that is not a function) the same kind of formula, $[a]_6 \mapsto [a]_4$, gave one class two values, and so defined no function.

The same situation will recur throughout this volume: for $\mathbb{Z}$ in this section, for $\mathbb{Q}$ in Section 2.4, and for $\mathbb{R}$ later in this volume. Each time, a set is a quotient $X/\sim$, and something is defined on it by a formula on elements of X . Rather than repeat the argument of *Sets, Relations, and Cardinality*, Proposition 2.5.5 for every formula, we separate it into two parts: a general lemma, proved here once, which turns a **check on representatives** into a function on classes; and the check itself, which is different for each formula and is all that remains to do each time.

A rule “ $[x] \mapsto$ something computed from x ” is called **well defined** when representatives of the same class always give the same result. The lemma below says that being well defined is enough, in three settings: a map from one quotient to another, a binary operation on a quotient, and a property of classes.

2.2.2 The lemma

A rule on classes is a function as soon as equivalent inputs give equivalent outputs.

Theorem 2.2.1. Functions on Classes

Let $\sim$ be an equivalence relation on a set X , and $\approx$ an equivalence relation on a set Y . Classes are taken for $\sim$ in X and for $\approx$ in Y .

- (a) Let $f: X \rightarrow Y$ be a function such that, **for all** $x, x' \in X$, $x \sim x'$ implies $f(x) \approx f(x')$. Then there is **exactly one** function $F: X/\sim \rightarrow Y/\approx$ with $F([x]) = [f(x)]$ for every $x \in X$.
- (b) Let $g: X \times X \rightarrow X$ be a function such that, **for all** $x, x', y, y' \in X$,

$$\begin{aligned} x \sim x' &\implies g(x, y) \sim g(x', y), \\ y \sim y' &\implies g(x, y) \sim g(x, y'). \end{aligned}$$

Then there is **exactly one** function $G: (X/\sim) \times (X/\sim) \rightarrow X/\sim$ with $G([x], [y]) = [g(x, y)]$ for all $x, y \in X$.

(c) Let $S \subseteq X$ be such that, for all $x, x' \in X$, $x \sim x'$ and $x \in S$ imply $x' \in S$. Let $\bar{S} := \{[x] : x \in S\} \subseteq X/\sim$. Then, **for every** $x \in X$, $[x] \in \bar{S}$ if and only if $x \in S$.

In words: (a) says that a map on elements that respects the two relations passes to a map on classes; (b) says that a binary operation that respects $\sim$ **in each argument separately** passes to an operation on classes; (c) says that a property that respects $\sim$ can be asked of a class, and the answer is the answer for any of its representatives. Clause (a) will give the negative of an integer, (b) its sum and product, and (c) the positive integers in Section 2.3.

Idea. A function is a graph with **exactly one** output for each input (Sets, Relations, and Cardinality, Definition 1.4.1). The obvious graph is the set of all pairs $([x], [f(x)])$. It has at least one output for each class, because every class is some $[x]$. The only danger is two outputs for one class, coming from two representatives x and x' of it; Sets, Relations, and Cardinality, Theorem 2.5.1 (b) turns “same class” into $x \sim x'$, the hypothesis turns that into $f(x) \approx f(x')$, and Sets, Relations, and Cardinality, Theorem 2.5.1 (b) turns it back into “same output”. For (b) the same plan works, once the two one-argument hypotheses are chained into one statement about both arguments by transitivity.

Proof. (a) Let

$$G_F := \{(C, D) \in (X/\sim) \times (Y/\approx) : C = [x] \text{ and } D = [f(x)] \text{ for some } x \in X\},$$

a set by specification (Sets, Relations, and Cardinality, Definition 1.1.3). We check the two clauses of Sets, Relations, and Cardinality, Definition 1.4.1. (Fn1): every $C \in X/\sim$ is $[x]$ for some $x \in X$ (Sets, Relations, and Cardinality, Definition 2.5.4), and then $(C, [f(x)]) \in G_F$. (Fn2): suppose $(C, D) \in G_F$ and $(C, D') \in G_F$, say $C = [x]$, $D = [f(x)]$, and $C = [x']$, $D' = [f(x')]$. Then $[x] = [x']$, so $x \sim x'$ by Sets, Relations, and Cardinality, Theorem 2.5.1 (b). By the hypothesis, $f(x) \approx f(x')$, so $[f(x)] = [f(x')]$ by Sets, Relations, and Cardinality, Theorem 2.5.1 (b), that is, $D = D'$. So F , the function with graph G_F and codomain $Y/\approx$, is a function $X/\sim \rightarrow Y/\approx$, and $F([x]) = [f(x)]$ because $([x], [f(x)]) \in G_F$.

For uniqueness, let $F' : X/\sim \rightarrow Y/\approx$ also satisfy $F'([x]) = [f(x)]$ for every x . Every $C \in X/\sim$ is some $[x]$, and then $F'(C) = [f(x)] = F(C)$. The two functions have the same domain and codomain, so $F' = F$ by Sets, Relations, and Cardinality, Proposition 1.4.1.

(b) First, for all $x, x', y, y' \in X$ with $x \sim x'$ and $y \sim y'$,

$$g(x, y) \sim g(x', y) \quad \text{and} \quad g(x', y) \sim g(x', y'),$$

by the first hypothesis (with y fixed) and the second (with x' fixed). By transitivity, (Eq3) of Sets, Relations, and Cardinality, Definition 2.5.1, $g(x, y) \sim g(x', y')$.

Now let G_G be the set of $(P, E) \in ((X/\sim) \times (X/\sim)) \times (X/\sim)$ such that $P = ([x], [y])$ and $E = [g(x, y)]$ for some $x, y \in X$, a set by specification. (Fn1): an element of $(X/\sim) \times (X/\sim)$ is a pair (C, D) of classes (Sets, Relations, and Cardinality, Definition 1.3.2), and $C = [x]$, $D = [y]$ for some $x, y \in X$ (Sets, Relations, and Cardinality, Definition 2.5.4); then $((C, D), [g(x, y)]) \in G_G$. (Fn2): suppose (P, E) and (P, E') lie in G_G , with $P = ([x], [y])$, $E = [g(x, y)]$, and $P = ([x'], [y'])$, $E' = [g(x', y')]$. From $([x], [y]) = ([x'], [y'])$ the characteristic property of pairs (Sets, Relations, and Cardinality, Definition 1.3.1) gives $[x] = [x']$ and $[y] = [y']$, so $x \sim x'$ and $y \sim y'$ by Sets, Relations, and Cardinality, Theorem 2.5.1 (b). By the first paragraph, $g(x, y) \sim g(x', y')$, so $E = E'$ by Sets, Relations, and Cardinality,

Theorem 2.5.1 (b). So G_G , with codomain $X/\sim$, defines a function G with $G([x], [y]) = [g(x, y)]$. Uniqueness is as in (a), by Sets, Relations, and Cardinality, Proposition 1.4.1.

(c) ($\Leftarrow$) If $x \in S$, then $[x] \in \bar{S}$ by the definition of $\bar{S}$. ($\Rightarrow$) If $[x] \in \bar{S}$, then $[x] = [x']$ for some $x' \in S$. By Sets, Relations, and Cardinality, Theorem 2.5.1 (b), $x \sim x'$, so $x' \sim x$ by (Eq2). The hypothesis, applied to $x' \sim x$ and $x' \in S$, gives $x \in S$.

This proves the theorem. ■

The functions F and G are said to be **induced** by f and g . In practice we write the conclusion of (a) as “the rule $[x] \mapsto [f(x)]$ is well defined”, and of (b) as “the operation $[x] * [y] := [g(x, y)]$ is well defined”, and the work is always the check of the hypotheses.

Remark. Each hypothesis has a job. Without the hypothesis of (c) the conclusion fails. On $\mathbb{N} \times \mathbb{N}$ with the relation $\sim$ of Definition 2.1.1, let $S := \{(a, b) : 0 < a\}$. Then $(1, 1) \in S$, so $[(1, 1)] \in \bar{S}$; and $[(0, 0)] = [(1, 1)]$, so $[(0, 0)] \in \bar{S}$, while $(0, 0) \notin S$. Membership in $\bar{S}$ does not tell us whether a particular representative lies in S . The hypotheses of (a) and (b) are needed in the same way, and the examples below show them failing.

2.2.3 Sum, product and negative of integers

To guess the formulas, borrow the school picture once more. If (a, b) records “ $a - b$ ” and (c, d) records “ $c - d$ ”, then school algebra gives

$$\begin{aligned} (a - b) + (c - d) &= (a + c) - (b + d), \\ (a - b)(c - d) &= (ac + bd) - (ad + bc), \\ -(a - b) &= b - a. \end{aligned}$$

These identities are a **heuristic**: they come from the school integers, which this chapter does not assume, and they are used only to find the definition. Each right side is again a difference of two natural numbers, so it can be recorded as a pair.

Definition 2.2.1. Sum, Product and Negative of Integers

For all $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$, let

$$\begin{aligned} [(a, b)] + [(c, d)] &:= [(a + c, b + d)], \\ [(a, b)] \cdot [(c, d)] &:= [(ac + bd, ad + bc)], \\ -[(a, b)] &:= [(b, a)]. \end{aligned}$$

The **sum** $+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ and **product** $\cdot: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ are the functions that Theorem 2.2.1 (b), with $X = \mathbb{N} \times \mathbb{N}$ and the equivalence relation $\sim$ of Proposition 2.1.1, induces from the maps g_+ , $g \cdot: (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \rightarrow \mathbb{N} \times \mathbb{N}$ given by the pairs on the right; the **negative** $-: \mathbb{Z} \rightarrow \mathbb{Z}$ is the function that Theorem 2.2.1 (a) induces from $(a, b) \mapsto (b, a)$. We also write xy for $x \cdot y$.

In words: to add integers, add representatives coordinatewise; to multiply, use the cross formula; to negate, swap the coordinates. All the arithmetic on the right happens in $\mathbb{N}$, where it is always

possible. The definition is legitimate only if the hypotheses of [Theorem 2.2.1](#) hold for the three maps on pairs; the next proposition checks them, and until then the three formulas are rules, not yet functions.

The move used in the proof is the one this chapter is built on.

Check on representatives, one argument at a time. To show that $[x] * [y] := [g(x, y)]$ is well defined, change x to an equivalent x' with y fixed, then change y to an equivalent y' with x' fixed. Each change is a computation at the level below, in $\mathbb{N}$ here; [Theorem 2.2.1](#) (b) joins the two by transitivity.

Proposition 2.2.2. The Operations on Integers Are Well Defined

The maps g_+ and g of [Definition 2.2.1](#) satisfy the hypotheses of [Theorem 2.2.1](#) (b), and the map $(a, b) \mapsto (b, a)$ satisfies those of [Theorem 2.2.1](#) (a), with $\sim$ on both sides. Hence the sum, product and negative of [Definition 2.2.1](#) are well-defined functions.

Idea. Each hypothesis is an equation in $\mathbb{N}$ to be derived from another. The given equation is the cross-sum equation for $(a, b) \sim (a', b')$; the target is the cross-sum equation for the two outputs. For the sum, adding $c + d$ to both sides of the given equation and rearranging is enough. For the product, the target has c and d in every term, so we multiply the given equation by c , and separately by d , and add the results; the rest is rearranging. Both formulas are unchanged when the two input pairs are swapped, so the second argument costs nothing.

Before reading on: why may we change one argument at a time, rather than both at once?

Proof. Let $(a, b), (a', b'), (c, d) \in \mathbb{N} \times \mathbb{N}$ with $(a, b) \sim (a', b')$, that is,

$$a + b' = b + a'. \quad (2.2.1)$$

All rearrangements below use [Theorem 1.5.3](#): commutativity and associativity of $+$, commutativity of $\cdot$, and distributivity.

Sum, first argument. We need $(a + c, b + d) \sim (a' + c, b' + d)$, that is, $(a + c) + (b' + d) = (b + d) + (a' + c)$. The left side is $(a + b') + (c + d)$, which by [Eq. 2.2.1](#) equals $(b + a') + (c + d)$, and that is the right side rearranged.

Product, first argument. We need

$$(ac + bd, ad + bc) \sim (a'c + b'd, a'd + b'c),$$

that is, the cross-sum equation

$$(ac + bd) + (a'd + b'c) = (ad + bc) + (a'c + b'd). \quad (2.2.2)$$

Multiply both sides of [Eq. 2.2.1](#) by c and use distributivity: $ac + b'c = bc + a'c$. Multiply both sides of [Eq. 2.2.1](#), read from right to left, by d : $bd + a'd = ad + b'd$. Adding these two equations,

$$(ac + b'c) + (bd + a'd) = (bc + a'c) + (ad + b'd).$$

The left side rearranges to the left side of Eq. 2.2.2, and the right side to its right side. This proves Eq. 2.2.2.

Second arguments. By commutativity in $\mathbb{N}$, $g_+((a, b), (c, d)) = (a + c, b + d) = (c + a, d + b) = g_+((c, d), (a, b))$, and likewise

$$g((a, b), (c, d)) = (ac + bd, ad + bc) = (ca + db, cb + da) = g((c, d), (a, b)).$$

So if $(c, d) \sim (c', d')$, then, by the first-argument case applied with the roles of the two pairs exchanged,

$$g((a, b), (c, d)) = g((c, d), (a, b)) \sim g((c', d'), (a, b)) = g((a, b), (c', d'))$$

for $g = g_+$ and $g = g_\cdot$. This is the second hypothesis of Theorem 2.2.1 (b).

Negative. The pair (b, a) is related to (b', a') when $b + a' = a + b'$, and that is Eq. 2.2.1 read from right to left. This is the hypothesis of Theorem 2.2.1 (a).

By Theorem 2.2.1 (b) and (a), the three rules define functions $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ and $\mathbb{Z} \rightarrow \mathbb{Z}$, as claimed. ■

The answer to the prompt is the first paragraph of the proof of Theorem 2.2.1 (b): two one-argument changes, $g(x, y) \sim g(x', y)$ and $g(x', y) \sim g(x', y')$, are joined by transitivity of $\sim$. Changing both at once is also possible, but the computation then mixes four equations in eight unknowns; one argument at a time keeps each computation to a single hypothesis.

2.2.4 Rules that fail

Every check happens in the hypotheses of the lemma. Here they fail, next to a rule where they hold.

Example. The first coordinate is not a function of the class

- (a) Does the rule $[(a, b)] \mapsto a$ define a function $\mathbb{Z} \rightarrow \mathbb{N}$?
- (b) Does the rule $[(a, b)] \mapsto [(a + 1, b)]$ define a function $\mathbb{Z} \rightarrow \mathbb{Z}$?
- (c) A student argues: “Each integer x has a pair with least first coordinate, by Theorem 1.6.2 applied to the non-empty set of first coordinates of the pairs in x ; call that least first coordinate $h(x)$. Then h is a function $\mathbb{Z} \rightarrow \mathbb{N}$, since each x determines its own least first coordinate. So $[(a, b)] \mapsto a$ is a function, namely h , with $h([(a, b)]) = a$ for every (a, b) .” Find the error.

Solution.

- (a) No. $(0, 2) \sim (1, 3)$, since $0 + 3 = 2 + 1$, so $[(0, 2)] = [(1, 3)]$ by Sets, Relations, and Cardinality, Theorem 2.5.1 (b). Read with the representative $(0, 2)$, the rule gives 0; read with $(1, 3)$, it gives 1. One input gets two values, and (Fn2) of Sets, Relations, and Cardinality, Definition 1.4.1 fails. The hypothesis of Theorem 2.2.1 (a), with $f(a, b) := a$ and equality on $\mathbb{N}$ as $\approx$ (so that $f(x) \approx f(x')$ means $f(x) = f(x')$), fails at $x = (0, 2)$, $x' = (1, 3)$.

(b) Yes. Let $(a, b) \sim (a', b')$, so $a + b' = b + a'$. Then

$$(a + 1) + b' = (a + b') + 1 = (b + a') + 1 = b + (a' + 1)$$

by Theorem 1.5.3 (b), (c), which is $(a + 1, b) \sim (a' + 1, b')$. By Theorem 2.2.1 (a), the rule is a function. In fact it is $x \mapsto x + [(1, 0)]$, since $[(a, b)] + [(1, 0)] = [(a + 1, b + 0)] = [(a + 1, b)]$.

(c) The conclusion is false, by (a), so some step fails. The function h is fine: the least first coordinate is computed from the set x alone. The failing step is the last clause, “ $h([(a, b)]) = a$ for every (a, b) ”. It holds only when (a, b) happens to be the pair with least first coordinate. The argument chose a particular representative to define h , and then used an **arbitrary** one. Counterexample to the step: $x = [(1, 3)] = [(0, 2)]$ contains $(0, 2)$, so $h(x) = 0$, while the representative $(1, 3)$ has first coordinate 1.

Warning. A formula that looks right need not be well defined. “ $[(a, b)] \cdot [(c, d)] := [(ac, bd)]$, like the sum” is not a definition: $(1, 0) \sim (2, 1)$, since $1 + 1 = 0 + 2$, but with $(c, d) = (1, 2)$ the outputs are $(1 \cdot 1, 0 \cdot 2) = (1, 0)$ and $(2 \cdot 1, 1 \cdot 2) = (2, 2)$, and $(1, 0) \not\sim (2, 2)$, since $1 + 2 \neq 0 + 2$. **And well defined is necessary, not sufficient.** The rule $[(a, b)] * [(c, d)] := [(ad + bc, ac + bd)]$ is well defined, since it is the negative of the product; but it gives $[(0, 1)] * [(0, 1)] = [(0 + 0, 0 + 1)] = [(0, 1)]$, so the “square” of the class of $(0, 1)$ is that class itself, not $[(1, 0)]$. Well-definedness says that a rule is a function; whether it is the right function is a separate question.

2.2.5 The natural numbers inside the integers

The integers were built to contain the natural numbers and more. They do not literally contain them: the natural number 0 is the empty set (Definition 1.5.1 (c)), while every integer is a non-empty class (Sets, Relations, and Cardinality, Theorem 2.5.1 (a)), so $0 \notin \mathbb{Z}$. What $\mathbb{Z}$ contains is a **copy** of $\mathbb{N}$, the classes in normal form $[(n, 0)]$, and the copy has the same arithmetic.

Proposition 2.2.3. The Natural Numbers Embed in the Integers

Let $\iota: \mathbb{N} \rightarrow \mathbb{Z}$, $\iota(n) := [(n, 0)]$.

(a) ι is injective, and for all $m, n \in \mathbb{N}$,

$$\iota(m + n) = \iota(m) + \iota(n), \quad \iota(mn) = \iota(m) \iota(n).$$

(b) For every $x \in \mathbb{Z}$, $x + \iota(0) = x$ and $\iota(1) \cdot x = x$. For every $(a, b) \in \mathbb{N} \times \mathbb{N}$, $[(a, b)] = \iota(a) + (-\iota(b))$.

(c) $\mathbb{Z} = \iota(\mathbb{N}) \cup \{-\iota(n) : n \in \mathbb{N}\}$.

Idea. The identities in (a) and (b) are computations with the formulas of Definition 2.2.1 in which at least one operand is some $\iota(n) = [(n, 0)]$, and its zero second coordinate makes most terms vanish. Injectivity and (c) are the two halves of Proposition 2.1.2: (b) of it says that different natural numbers give different classes, and (a) says that every class is in normal form.

Proof. (a) If $\iota(m) = \iota(n)$, then $[(m, 0)] = [(n, 0)]$, so $m = n$ by Proposition 2.1.2 (b); hence ι is injective (Sets, Relations, and Cardinality, Definition 1.4.3). By Definition 2.2.1,

$$\iota(m) + \iota(n) = [(m + n, 0 + 0)] = [(m + n, 0)] = \iota(m + n),$$

since $0 + 0 = 0$ (Definition 1.5.1 (a)), and

$$\iota(m) \iota(n) = [(mn + 0 \cdot 0, m \cdot 0 + 0 \cdot n)] = [(mn, 0)] = \iota(mn),$$

since $m \cdot 0 = 0$ (Definition 1.5.1 (b)), $0 \cdot n = 0$ (Theorem 1.5.3 (e)) and $k + 0 = k$.

(b) Let $x = [(a, b)]$. Then $x + \iota(0) = [(a + 0, b + 0)] = [(a, b)] = x$, and

$$\iota(1) \cdot x = [(1 \cdot a + 0 \cdot b, 1 \cdot b + 0 \cdot a)] = [(a, b)] = x,$$

by Theorem 1.5.3 (e) ($1 \cdot n = n$, $0 \cdot n = 0$) and $n + 0 = n$. Finally, $-\iota(b) = -[(b, 0)] = [(0, b)]$, so $\iota(a) + (-\iota(b)) = [(a + 0, 0 + b)] = [(a, b)]$, using $0 + b = b$ (Theorem 1.5.3 (a)).

(c) ($\supseteq$) Both sets on the right consist of integers. ($\subseteq$) Let $x \in \mathbb{Z}$. By Proposition 2.1.2 (a), $x = [(k, 0)]$ or $x = [(0, k)]$ for some $k \in \mathbb{N}$. In the first case $x = \iota(k)$. In the second, $x = [(0, k)] = -[(k, 0)] = -\iota(k)$ by Definition 2.2.1. So x lies in the right side. ■

Identification. From now on we write n for $\iota(n)$ and regard $\mathbb{N}$ as a subset of $\mathbb{Z}$. This is a convenient abuse of notation, and (a) makes it honest: because ι is injective, different natural numbers stay different; because ι preserves $+$ and $\cdot$, a sum or product of natural numbers is the same whether computed in $\mathbb{N}$ or in $\mathbb{Z}$. One could rebuild $\mathbb{Z}$ so that it contains $\mathbb{N}$ literally, by putting each n in place of $\iota(n)$, but nothing later needs it. The order of $\mathbb{N}$ is matched to an order on $\mathbb{Z}$ in Section 2.3.

With this convention, (b) reads $[(a, b)] = a + (-b)$: the pair (a, b) records the difference it was meant to record. The notation $a - b$ is defined in Section 2.3, where $x - y := x + (-y)$ is set up in every ring at once. Clause (c) reads

$$\mathbb{Z} = \mathbb{N} \cup \{-n : n \in \mathbb{N}\},$$

which is word for word the definition of the integers in *Sets, Relations, and Cardinality*, Section 2.1. There it was a definition inside the familiar real numbers; here it is a theorem about a set built from ω . The positive integers keep the definition of *Sets, Relations, and Cardinality*, Section 2.1,

$$\mathbb{Z}_{>0} := \{n \in \mathbb{N} : n \neq 0\},$$

which mentions only $\mathbb{N}$, and so is now a subset of $\mathbb{Z}$. In particular $5 + x = 3$ has the solution $x = [(0, 2)] = -2$ in $\mathbb{Z}$, since $[(5, 0)] + [(0, 2)] = [(5, 2)] = [(3, 0)]$ by Proposition 2.1.2 (a).

Quick check. Compute $[(2, 5)] \cdot [(4, 1)]$ from Definition 2.2.1, and write the two factors and the product as n or $-n$ with $n \in \mathbb{N}$.

Solution. $[(2, 5)] \cdot [(4, 1)] = [(2 \cdot 4 + 5 \cdot 1, 2 \cdot 1 + 5 \cdot 4)] = [(13, 22)]$. By Proposition 2.1.2 (a): $5 = 2 + 3$, so $[(2, 5)] = [(0, 3)] = -3$; $4 = 1 + 3$, so $[(4, 1)] = [(3, 0)] = 3$; and $22 = 13 + 9$, so $[(13, 22)] = [(0, 9)] = -9$. So the product of -3 and 3 is -9 , as school predicts; here it is a

computation in $\mathbb{N}$, not a rule of signs.

The integers now have a sum, a product and a negative, each a function on classes, and they contain a copy of $\mathbb{N}$ with its arithmetic. Section 2.3 checks that these operations obey the usual laws, by reducing each law to a law of $\mathbb{N}$, and defines the order.

2.2.6 Exercises

2.2.6.1 A. Check your understanding

Exercise. A1

These questions are about the proof of [Proposition 2.2.2](#).

- Which hypothesis of [Theorem 2.2.1](#) (b) does the computation leading to [Eq. 2.2.2](#) verify?
- Run that computation with $(a, b) = (1, 3)$, $(a', b') = (4, 6)$ and $(c, d) = (2, 0)$: check that $(a, b) \sim (a', b')$, compute both outputs, and check that they are equivalent.
- Where in the proof are the laws of arithmetic in $\mathbb{N}$ used?
- Give the idea of the proof in two sentences.

Solution.

- The first: for all x, x', y , $x \sim x'$ implies $g.(x, y) \sim g.(x', y)$, with $x = (a, b)$, $x' = (a', b')$, $y = (c, d)$.
- $1 + 6 = 7 = 3 + 4$, so $(1, 3) \sim (4, 6)$. The outputs are

$$\begin{aligned} (ac + bd, ad + bc) &= (2 + 0, 0 + 6) = (2, 6), \\ (a'c + b'd, a'd + b'c) &= (8 + 0, 0 + 12) = (8, 12), \end{aligned}$$

and $2 + 12 = 14 = 6 + 8$, so they are equivalent. The two intermediate equations are $ac + b'c = bc + a'c$, here $2 + 12 = 6 + 8$, and $bd + a'd = ad + b'd$, here $0 = 0$, since $d = 0$. Both outputs are representatives of -4 , and indeed $(-2) \cdot 2 = -4$.

- In every rearrangement: commutativity and associativity of $+$ (to regroup the four-term sums), distributivity (to multiply [Eq. 2.2.1](#) by c and by d), and commutativity of $\cdot$ and $+$ (in the second-argument step, to see that both formulas are symmetric in the two input pairs).
- A change of representative in one argument is an equation in $\mathbb{N}$, and multiplying it by c and by d and adding gives exactly the cross-sum equation for the two products. The second argument follows by symmetry of the formula, and transitivity (inside [Theorem 2.2.1](#) (b)) combines the two changes.

2.2.6.2 B. Practice

Exercise. B1: Two rules that pass the check

Prove that each rule defines a function $\mathbb{Z} \rightarrow \mathbb{Z}$, and identify it in terms of the operations of [Definition 2.2.1](#).

- (a) $[(a, b)] \mapsto [(b, a)]$.
- (b) $[(a, b)] \mapsto [(a + b, a + b)]$.

Solution.

- (a) Let $(a, b) \sim (a', b')$, that is, $a + b' = b + a'$. The target $(b, a) \sim (b', a')$ is $b + a' = a + b'$, the same equation read from right to left. By [Theorem 2.2.1](#) (a), the rule is a function. It is the negative $x \mapsto -x$ of [Definition 2.2.1](#).
- (b) Every output is the zero class: $(a + b, a + b) \sim (0, 0)$, since $(a + b) + 0 = (a + b) + 0$. So for $(a, b) \sim (a', b')$ the outputs $(a + b, a + b)$ and $(a' + b', a' + b')$ are both related to $(0, 0)$, hence to each other by (Eq2) and (Eq3) of Proposition 2.1.1, and [Theorem 2.2.1](#) (a) applies. The function is the constant map $x \mapsto 0$, where $0 = \iota(0) = [(0, 0)]$. In terms of [Definition 2.2.1](#) it is $x \mapsto x + (-x)$, since $[(a, b)] + [(b, a)] = [(a + b, b + a)] = [(a + b, a + b)]$ by Theorem 1.5.3 (b).

Exercise. B2: Determine which

Determine which of the following rules define a function. Justify your answer.

- (a) $\mathbb{Z} \rightarrow \mathbb{N}$, $[(a, b)] \mapsto a + b$.
- (b) $\mathbb{Z} \rightarrow \mathbb{Z}$, $[(a, b)] \mapsto [(2a, 2b)]$.
- (c) $\mathbb{Z} \rightarrow \mathbb{Z}$, $[(a, b)] \mapsto [(a^2, b^2)]$, where $n^2 := n \cdot n$.

Solution.

- (a) No. $[(0, 0)] = [(1, 1)]$, since $0 + 1 = 0 + 1$, but the rule gives $0 + 0 = 0$ for the first representative and $1 + 1 = 2$ for the second.
- (b) Yes. If $a + b' = b + a'$, then by distributivity (Theorem 1.5.3 (d))

$$2a + 2b' = 2(a + b') = 2(b + a') = 2b + 2a',$$
 which is $(2a, 2b) \sim (2a', 2b')$; [Theorem 2.2.1](#) (a) applies. The function is $x \mapsto x + x$: $[(a, b)] + [(a, b)] = [(a + a, b + b)]$, and $2n = (1 + 1)n = n + n$ by $1 + 1 = 2$ (Definition 1.5.1 (c)) and Theorem 1.5.3 (d), (e).
- (c) No. $[(0, 1)] = [(1, 2)]$, since $0 + 2 = 1 + 1$. The rule gives $[(0, 1)]$ for the first representative and $[(1, 4)]$ for the second, and $(0, 1) \not\sim (1, 4)$, since $0 + 4 = 4 \neq 2 = 1 + 1$.

2.2.6.3 C. Going deeper

Exercise. C1: Properties of classes, and an operation that half works

- (a) Prove [Theorem 2.2.1](#) (c), and give an example, different from the one in the remark after the theorem, of a subset $S \subseteq \mathbb{N} \times \mathbb{N}$ for which its conclusion fails for $\sim$ of Definition 2.1.1.
- (b) Give an example of an equivalence relation $\sim$ on $\mathbb{N}$ and a function $g: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ such that the first hypothesis of [Theorem 2.2.1](#) (b) holds and the second fails. Check each property, and show that no function G as in the conclusion of (b) exists for your

example.

Solution.

- (a) *Proof.* Let $x \in X$. If $x \in S$, then $[x] \in \bar{S}$ by the definition of $\bar{S}$. Conversely, if $[x] \in \bar{S}$, there is $x' \in S$ with $[x] = [x']$; then $x \sim x'$ (Sets, Relations, and Cardinality, Theorem 2.5.1 (b)), so $x' \sim x$ by symmetry, and the hypothesis on S , applied to $x' \sim x$ and $x' \in S$, gives $x \in S$.

Example. Let $S := \{(a, b) \in \mathbb{N} \times \mathbb{N} : a = 0\}$. Then $(0, 0) \in S$, so $[(0, 0)] \in \bar{S}$; and $[(1, 1)] = [(0, 0)]$, so $[(1, 1)] \in \bar{S}$, but $(1, 1) \notin S$. The hypothesis fails at $(0, 0) \sim (1, 1)$. Any example must contain a pair of S and an equivalent pair outside S , since that is exactly the negation of the hypothesis.

- (b) *Example.* On $\mathbb{N}$, let $x \sim y$ mean “ $x = 0$ if and only if $y = 0$ ”. This is an equivalence relation: it says that x and y have the same value under the function sending 0 to 0 and every other number to 1, so it is an equivalence relation by Sets, Relations, and Cardinality, Example (The fibers of a function). Its two classes are $\{0\}$ and $\mathbb{N} \setminus \{0\}$. Let

$$g(x, y) := \begin{cases} x & \text{if } y = 1, \\ 0 & \text{if } y \neq 1. \end{cases}$$

First hypothesis holds. Let $x \sim x'$ and $y \in \mathbb{N}$. If $y = 1$, then $g(x, y) = x \sim x' = g(x', y)$. If $y \neq 1$, both values are 0, and $0 \sim 0$.

Second hypothesis fails. $1 \sim 2$, since neither is 0; but $g(5, 1) = 5$ and $g(5, 2) = 0$, and $5 \not\sim 0$.

No induced G . If $G([x], [y]) = [g(x, y)]$ held for all x, y , then, since $[1] = [2]$, we would get $[5] = [g(5, 1)] = G([5], [1]) = G([5], [2]) = [g(5, 2)] = [0]$, and $[5] \neq [0]$ because $5 \not\sim 0$.

What any example must have. (i) $\sim$ is not equality: some class has two elements $y \sim y'$ with $y \neq y'$, else the second hypothesis holds trivially. (ii) $\sim$ has at least two classes, else every two outputs are related and both hypotheses hold. (iii) For some x and some $y \sim y'$, the values $g(x, y)$ and $g(x, y')$ lie in different classes, while for every y , changing x within its class never moves $g(x, y)$ out of its class. A different answer can be checked against (i)–(iii).

Exercise. C2: One at a time or both at once

Let $\sim$ be an equivalence relation on X and $g: X \times X \rightarrow X$ a function. Prove that the hypotheses of Theorem 2.2.1 (b) hold if and only if, for all $x, x', y, y' \in X$,

$$x \sim x' \text{ and } y \sim y' \implies g(x, y) \sim g(x', y').$$

Name the property of $\sim$ that each direction uses.

Solution. ($\implies$) Let $x \sim x'$ and $y \sim y'$. The first hypothesis, with y fixed, gives $g(x, y) \sim g(x', y)$; the second, with x' fixed, gives $g(x', y) \sim g(x', y')$. By **transitivity** (Eq3), $g(x, y) \sim g(x', y')$. This direction is the first paragraph of the proof of Theorem 2.2.1 (b).

($\impliedby$) Let $x \sim x'$ and $y \in X$. By **reflexivity** (Eq1), $y \sim y$, so the displayed condition with $y' = y$ gives $g(x, y) \sim g(x', y)$: the first hypothesis. Likewise $x \sim x$ and $y \sim y'$ give $g(x, y) \sim g(x, y')$: the second.

So the two forms are interchangeable. The one-at-a-time form is the one to check, because each check involves a single hypothesis $x \sim x'$; the both-at-once form is the one the proof of the lemma uses.